International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.2, pp : 139 – 143 1 Feb 2014

# Public Key Encryption without using Certificate based on Identity Based Cryptography

**S.Kuzhalvaimozhi[1], Dr.G.Raghavendra Rao[2]**

[1] Associate Professor, Dept of ISE, National Institute of Engineering, Mysore, Karnataka, India.
Email: kuzhali_mozhi@yahoo.com
[2] Professor& Head, Dept of CSE, National Institute of Engineering, Mysore, Karnataka, India.

***Abstract: It has been proven for many years that security for digital information can be attained by the cryptography techniques. Identity based cryptography (IBC) is an emerging area in cryptography schema. Identity based cryptography is the new system which reduces the key management process in traditional public key infrastructures (PKI). The main drawbacks of the traditional Public key cryptosystems (PKC) are use of very long keys, the high cost of the infrastructure and the difficulty in managing multiple parties involved in the process. In PKC digital certificates are used to connect an identity of a person or a machine to a public key. IBC is the extension of public key crypto system. The public keys of IBC system created from any arbitrary unique information like identities, or strings derived from their identities. Any public information such as the e-mail address, name, phone numbers, etc., can be used as a public key. The algorithm for IBC resolves the problem of getting the public key of a user and checking the validity of certificate and helps to avoid the trust problems encountered in traditional certificate based PKI. Two users can communicate in secured manner without the need for exchanging of public or private keys and without keeping any key directories to store the public keys. In this paper we are proposing an algorithm that uses the Identity Based Cryptosystem and its applications in various fields.***

Keywords: Identity based cryptography, Public key infrastructures, Digital information security and certificate based PKI.

## 1. Introduction

In the recent revolution in the field of information technology and internet made protection of the date as important research. Because the date communicated between the valid user can be seen by others. The concept of Public Key Encryption, suggested by Diffie and Hellman, started a revolution in cryptography. This system facilitated the two parties without ever having met before, want to talk confidently over insecure channels to encrypt their message.

Certificates [8] are used in public key crypto system to offer a guarantee of the relationship between public keys and the identities. This assurance on a public key is delivered in the form of certificate which is granted with a signature by a Certification Authority (CA).

A sender can able to encrypt a message for a recipient only when the recipient has acquired a certificate before the communication of the message and the certificate should be available to the sender. In traditional public key cryptography the main difficulty is not in choosing or implementing the secure algorithms but is to develop an infrastructure to maintain the authenticity of a user's public key.

The identity-based cryptography is a new research area in Public Key Crypto system. The IBC algorithm helps to avoid the requirement of digital certificates. Shamir[1] first proposed technique known as identity-based public key cryptography to address the limitations of PKI. Since then, many ID-based encryption [2, 3] and signature schemes have been proposed. The main idea of Identity based cryptosystems is that the identity information of each user works as his/her public key.

Identity Based Cryptography (IBC) does not need certificates, as public keys are calculated from public identifiers. The size of an identifier may be smaller compared to the size of a certificate. This provides a considerable advantage in terms of communication cost savings, mostly in applications where multiple certificates require to be transmitted between two nodes.

The public key of the parties involved in the communication is calculated directly their personal identity information such as e-mail address, name rather than being calculated from a certificate issued by a Certificate Authority. This type of algorithm is mainly useful for the situation where efficient key management and moderate security are required. The security mechanism obtained by the IBC is equal to the traditional public key algorithms. The concepts of regular

public key encryption are illustrated as shown in Figure1. and the Identity Based Crypto System in Figure 2.

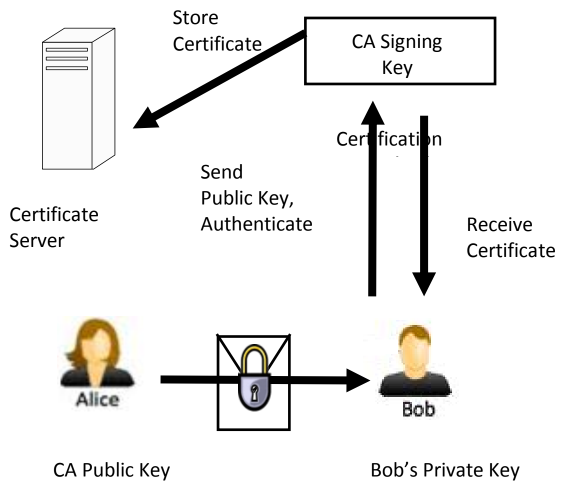


Figure 1: Traditional Public Key Cryptosystem

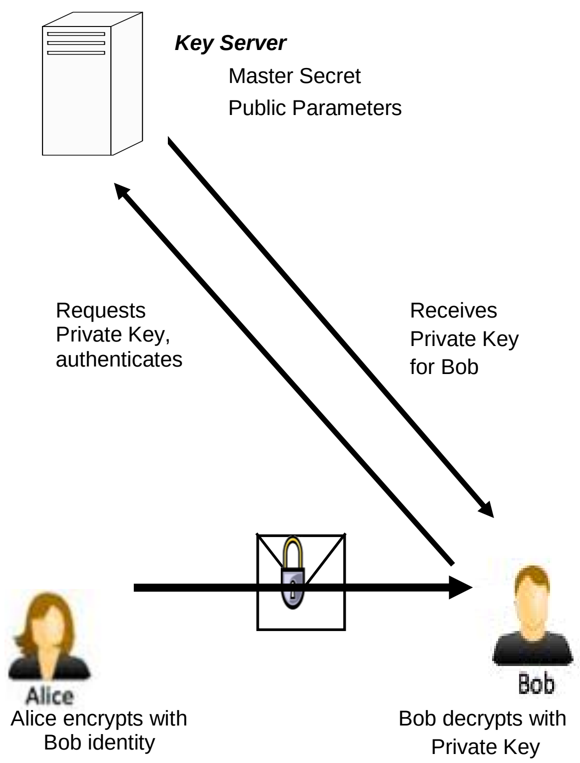


Figure 2**:** IBC Cryptosystem

Two users, for example Alice send a message to Bob in the encrypted format. The main objective of this communication is the message should be authenticated and arrive at the receiver(Bob) securely. In traditional Public key cryptosystems as shown in Figure 1:, Before the encryption of the message, the sender of the message be in agreement on a secret key with the receiver. Then the sender(Alice) encrypt the message and send the encrypted message to the receiver(Bob).

Bob gets the certificate from CA for his private key and then he decrypts the message. The sender cannot start the encryption of the message if the receiver had not generate the private and public key pair which needs to be uploaded to the key server.

But in IBC scheme as shown in Figure 2:, Bob can uses his identity like e-mail address (*Bob@abc.com*) as his public key. The private key is generated from Key Generation Authority for the public key. The private key is send to Bob only when bob proves his identity.

## 2. Related Work

Original system developed by Shamir [1] was based upon the popular cryptosystem RSA encryption. The system proposed by Shamir is a signature-only system. He was unable to extend the proposed system to an encryption system. After the development of first IBC system, a many IBE systems were created. But the all systems suffered with the limitations on huge amount of calculations. The amount of calculations done by the PKG was huge.

Two new proposals were published in 2001 which is an improved version of previous algorithm. The algorithm developed by Cocks is based upon quadratic residues [3,4]. The encryption algorithm used in the Cocks scheme used bit by bit encryption of the message. The size of the encrypted message is increased. In this system 1024 bit modulus and 128 bit key was used. After encryption data size was nearly 16K. But for the modern network technology this will not be big overhead.

Weil pairing is used in the system developed by Dan Boneh and Matt Franklin [2] in 2003. The concept of Bilinear maps between groups used in Pairing-based systems. Bilinear maps provide a relationship between groups and hashes of the identity generate the encryption scheme.

The Identity Based Encryption developed by C.Gentry uses the hybrid approach which uses certificate approach with identity based encryption. Al-Riyami and Paterson developed a method for Certificateless Public Key Cryptography.

## 3. Bilinear Pairing

Bilinear pairing is an important primitive for many cryptographic schemes. Many elegant cryptographic schemes

have been formulated utilizing the properties of these bilinear pairings.

Let G1 be an additive group of prime order q, generated by p, and let G2 be a multiplicative group with the same order q. We assume that there is a bilinear map e from $G1 \times G1 \rightarrow G2$ with the following properties:

(1) Bilinearity: Which means that given elements A1, A2, A3 ϵ G1 , we have that

$e(A1 + A2, A3) = e(A1,A3) \times e(A2,A3)$ and
$e(A1, A2 + A3) = e(A1, A2) \times e(A1, A3)$.

In particular, for $e(aA1, bA2) = e(A1, A2)^{ab}$, a,b ε Z*q where Zp denotes all positive integer which is less than p. Z*q denotes multiplicative group modulo p.

(2) Non-degeneracy: Which means that there exists A1, A2 ε G1 such that $e(A1, A2) \neq 1G2$ , where 1G2 is the identity of G2.

(3) Computability: Which means that there exists an efficient algorithm to compute e(A1, A2) A1, A2 ε G1.

Decision Diffie-Hellman is easy: The Decision Diffie-Hellman problem (DDH). Given aP, bP, cP ε G1. If we want to decide whether cP = abP, we can easily determine by checking e(P, cP) = e(aP, bP).

Computational Diffie-Hellman is hard: The Computational Diffie-Hellman problem (CDH). Given P, aP, bP ε G1, if we want to compute abP ε G1, it is assume to be hard.

Since the Decision Diffie-Hellman problem (DDH) in G1 is easy, we cannot use DDH to build our cryptosystems. Instead, the security of our IBE system is based on a variant of the Computational Diffie-Hellman assumption (CDH).

## 4. Applications of IBC

There are many notable real world applications based on IBC[9]. In the e-cash, e-commerce and other e-transaction applications, the main concern is the implementation of the confidentiality of network communications. Implementation of confidentiality becomes simpler because of the development of Identity Based Cryptosystem. IBC permits the secured network business and the users to validate the authenticity and integrity of their transactions.

Because of the increase in global electronic, improved IBC algorithms will have to be created to protect the sensitivity of the data in the business transactions. There are many examples of e-transactions via internet the sensible medium such as credit card transaction details, bank account details, health details, personal details, tax records can be protected using IBC. The Identity based cryptosystem can be used in following areas where protection of vital data is very important.

### 4.1 Electronic Voting

Electronic voting is currently used in many applications for example in national ballot, companies, etc. The existing systems for electronic voting are fraught with difficulties and flaws. Thus allows malicious users to tamper with the votes. The ID-based ring signature scheme [8,11] can be used for applications like electronic voting, which is more efficient and practical.
Using ID based ring signatures [7], the voting authority can verify that someone in the group sent the vote, but will not be able to find the exact person. The identification based cryptography used in electronic voting does not require public keys storage or the public key binding management. The required resource is only the computing time to develop the cryptographic operations. The protocol used for e-voting need two cryptographic primitives, encryption and signature.

### 4.2 Grid Security

The majority of current grid security system uses public key infrastructure to authenticate identities and to secure resource allocation for the grid members. In comparison with traditional PKI, the IBC may offer more flexible and lightweight key usage and management approaches within grid security infrastructures. To provide the security to grid environment, the IBC is well suited. The IBC can be used in dynamic grid environment, because the system is certificate free and flexible

To support well with the demands of grid computing the Identity based cryptography has some attractive properties. Identity based key agreement protocol fits nicely with the Grid Security Infrastructure [7], [10] and provides a more lightweight secure job submission environment for grid users. Single sign on and delegation services are also supported in a very natural way in identity based architecture.

### 4.3 Email Encryption

Nowadays Email is the main medium for the communication of the business, used inside the organization as well as outside to business partners and customers. As email usage increases, the main concern is to protect the privacy of email. Thus e-mail messages must be protected by some method of security. IBE utilize the proven encryption technologies to provide well

built security for the most sensitive email communications which can be easily managed.

Using IBE, secure messages can be sent to any recipient, without first requiring the recipient to take any special action. Encrypted emails can be sent to inside or outside the organization just like a regular email with no additional steps required by the sender or the receiver. Once the recipient receives a secure email, a simple connection to the appropriate key server to authenticate and receive the decryption key is the only step necessary before he or she can successfully access the secure message.

IBE technology does not require to store user certificates or keys, thus needs less operational overhead. IBE is providing end-to-end security combined with policy-based encryption for the email. The implementations scale to several hundred thousand internal users and it easily integrates into the existing environment.

**4.4 Securing Mobile Phone Calls**

The current encryption schemes available in 2G and 3G technology, only encrypt the calls between the mobile phone and the base station. Anywhere in the network, an attacker can located in between the two base stations. They can usually intercept calls without any greater effort. In addition, the base stations of GSM are not authenticated. An attacker can forged as a base station. So they can catch phone calls in the vicinity. To prevent such attacks end to end protection of mobile phone calls is required.

The conventional Public Key Infrastructure solution for this type of problem is complex The security solutions are difficult to implement for the network providers and for the users. Identity-based cryptography proposes an algorithm to end-to-end encryption for mobile telephone calls [11,12, 13] in which the telephone numbers of the customers can be are used as the public keys to secure the communication channel, thus making the cryptographic security procedure as easy as making a telephone call.

There two major benefits are there by using the telephone numbers as public keys.

1. The caller knows the number to be called; the caller also knows the public key. So he does not require a separate public key lookup or certification infrastructure.

2. Telephone numbers are simple to know, such that there is no need to instruct users about the relation between a telephone number used as a public key and the corresponding certificates. The IBC algorithm provides two mobile phones to carry out a key agreement through an untenable channel and different telephone providers using telephone numbers as public keys.

## 5. Identity Based Encryption algorithm

The algorithm for Identity Based Encryption system contains four basic steps in its construction:

1. *System Setup:* Before the encryption of the message the parameters used in encryption process is decided by the third party. The trusted third party is responsible for the creation and management of public parameters and keys. This trusted third party is usually called as Trusted Authority (TA).
   - Selects two groups G1 and G2 of order q, a bilinear map e from $G1 \times G1 \rightarrow G2$
   - Selects generator P from G1
   - picks a master secret key ms where $ms \in Z^*q$
   - selects two Cryptographic hash functions *hf1* and *hf2*
   - selects $hf1 : \{0,1\}^* \rightarrow G1^*$
   - selects $hf2 : G2 \rightarrow \{0,1\}^n$
   - calculates Pub=ms • P. The operator • is multiplication of integers with points on elliptic curve.
   - publishes the system parameter $\{ G1, G2, hf1, hf2, q, P, e, Pub, n \}$ to all the users and keeps the key ms secret. In this step calculating $ms \bullet P$ is easy, but for a given P finding the value of ms is practically impossible.

2. *Encryption*: This algorithm uses the receiver‘s identity ($ID_i$) as a public key to encrypt the messages. When a sender wishes to encrypt a message by computing or obtaining the public key and then encrypting a plaintext message *msg* with to obtain ciphertext C.
   - Calculates $K_1 = hf1(ID_i);$
   - Selects a random number $r_1 \in Z^*q$
   - Calculates $c1= r_1 \cdot P$
   - Calculates
     $c2= msg \circ hf2(e(r_1 \cdot K_1, Pub))$
   - Sends the ciper text $C=<c1,c2>$ to the receiver

3. *Key Extraction*: When the receiver wishes to decrypt the encrypted message C, he authenticates himself to the TA and obtains the private key that he uses to decrypt messages.
   - Calculates $K_1 = hf1(ID_i)$
   - Proves the identity with TA
   - TA calculates $Pri = ms \cdot K_1$
   - Send the private key *Pri* to the receiver

4. *Decryption*: When the receiver has *C* and *Pri* he decrypts C to obtain the plaintext message *msg*

- Calculates msg = c2 $\circ$ *hf2(e(pri,c1))*
  *where c2= msg* $\circ$ $hf2(e(r_1 \cdot K_1, Pub))$
- msg = c2 $\circ$ *hf2(e(pri,c1))*

*Proof:*

$= msg \circ hf2(e(r_1 \cdot K_1, Pub)) \circ hf2(e(pri,c1))$

Where $Pri = ms \cdot K_1$ and $c1 = r_1 \cdot P$

$= msg \circ hf2(e(r_1 \cdot K_1, Pub)) \circ hf2(e(ms \cdot K_1, r_1 \cdot P)$

Using bilinear property $e(aA1, bA2) = e(A1, A2)^{ab}$

$= msg \circ hf2(e(r_1 \cdot K_1, Pub)) \circ hf2(e(K_1, P))^{ms \cdot r1}$

$= msg \circ hf2(e(r_1 \cdot K_1, Pub)) \circ hf2(e(K_1, ms \cdot P)^{r1}$

$= msg \circ hf2(e(r_1 \cdot K_1, Pub)) \circ hf2(e(r_1.K_1, ms \cdot P)$

here $Pub=ms.P$

$= msg \circ hf2(e(r_1 \cdot K_1, Pub)) \circ hf2(e(r_1.K_1, Pub)$

$= msg$

## Conclusions

In this paper the algorithm is discussed on Identity based cryptosystems which simplify key management and avoid the use of digital certificate by allowing public key be publicly derivable from human rememberable information on its owner. This scheme can greatly reduce the complexity of sending encrypted messages. This algorithm can be useful for many applications where data security is highly important.

## References


*i.A. Shamir, Identity-based Cryptosystems and Signature Schemes, In Advances in Cryptology-Crypto'84, LNCS vol. 196, Springer-Verlag,1984, pp. 47-53.*

*ii.D. Boneh, X. Boyen, "Secure Identity Based Encryption Without Random Oracles", In Advances in Cryptology-Crypto'04, LNCS 3152, pp. 443-459, Springer-Verlag, 2004.*

*iii.D. Boneh, M. Franklin, "Identity-based Encryption from the Weil pairing", SIAM J. of Computing, 32(3):586-615, 2003. Extended abstract in Advances in Crptology-Crypto'01, LNCS 2139, pp.213-229, Springer- Verlag, 2001*

*iv.C. Cocks, An Identity Based Encryption Scheme Based on Quadratic Residues, International Conference on Cryptography and Coding-Proceedings of IMA, LNCS 2260,pp. 360-363, Springer-Verlag,2001.*

*v.Identity-Based Encryption: a Survey, RSA Laboratories Cryptobytes, Vol. 6, No. 1, Spring 2003.*

*vi.C.Gentry, Certificate Based Encryption and the Certificate Revocation Problem, EUROCRYPT 2003, LNCS 2656, pp. 272-293, 2003*

*vii.Lingling WANG, Guoyin ZHANG, Chunguang MA. A survey of ring signature Springer-Verlag, 2008*

*viii.C. Ellison , B. Schneier. Ten risks of PKI: What you're not being told about public key infrastructure. Computer Security Journal, 16(1):1–7, 2000.*

*ix.Yanjiong Wang, Qiaoyan Wen, Hua Zhang, "A Single Sign-On Scheme for Cross Domain Web Applications Using Identity-Based Cryptography," Networks Security, Wireless Communications and Trusted Computing, International Conference on, pp. 483-485, 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010*

*x.B. G. Lee, D. H. Choi, H. G. Kim, S. W. Sohn, and K. H. Park, "Mobile IP and WLAN with AAA authentication protocol using Identity-based cryptography," in Proc. IEEE ICT'03, vol. 1, pp. 597-603, 23 Feb. 2003.*

*xi.Gina Gallegos-Garcia, Roberto Gomez-Cardenas, Gonzalo I. Duchen-Sanchez, "Electronic Voting Using Identity Based Cryptography," International Conference on the Digital Society, pp. 31-36, 2010 Fourth International Conference on Digital Society, 2010*

*xii.Matthew Smith, Christian Schridde, Bjorn Agel, Bernd Freisleben, "Identity-Based Cryptography for Securing Mobile Phone Calls," Advanced Information Networking and Applications Workshops, pp. 365-370, 2009 International Conference on Advanced Information Networking and Applications Workshops, 2009*

*xiii.Crampton, J., Lim, H. W., and Paterson, K. G. 2007." What can identity-based cryptography offer to web services?", In Proceedings of the 2007 ACM Workshop on Secure Web Services (Fairfax, Virginia, USA, November 02 - 02, 2007). SWS ' 07. ACM, New York, NY, 26-36.*